Message

From: Shannon Newberry [redacted]@google.com]
Sent: 8/25/2018 2:59:13 PM
To: Jamie Rosenberg [redacted]@google.com]
CC: Edward Cunningham [redacted]@google.com]; Tristan Ostrowski [redacted]@google.com]; Lydia Ash [redacted]@google.com]; Hiroshi Lockheimer [redacted]@google.com]; Dave Kleidermacher [redacted]@google.com]; Purnima Kochikar [redacted]@google.com]; Mike Hochberg [redacted]@google.com]; Sameer Samat [redacted]@google.com]; William Luh [redacted]@google.com]; Tian Lim [redacted]@google.com]; Colin Smith [redacted]@google.com]; Kareem Ghanem [redacted]@google.com]
Subject: Re: ATTORNEY CLIENT PRIVILEGED Fortnight task force

privileged and confidential

Hi all,

The Android Central article has been updated. Under Tim's quote, the reporter included the following:

Google may have jumped the shark in Epic's mind, but this course of action clearly followed Google's policy for disclosure of 0day vulnerabilities.

Since most stories link to the Android Central piece, this update will help. I've also been sharing our background points and asking contacts I know to update stories with our security vulnerability policy.

Few new pieces also popped up overnight worth highlighting:

9to5Google: Google-found security flaw quickly proves why Fortnite should be on the Play Store
"To Epics' credit, version 2.1 of the Installer that fixed the issue was rolled out the very next day. The game developer requested that Google wait 90 days before disclosing the issue, but Google followed its well-known stringent policy of detailing the vulnerability as it had been seven days since the patch was made available."

Telegraph (opinion piece): Fortnite app allowed hackers to secretly install anything on Android phones

This story is also still on Techmeme this morning.

I'm not planning on updating our statement, but will continue to send our points on background to ensure this messaging about the timeframe clarifies the claim Epic is making.

Will continue to monitor and update this group as things evolve. Thanks to Ed, Tristan and Dave for the help (especially in the last 12 hours) so I could update our messaging to ensure this lands news still lands cleanly.

Thanks,
Shannon

On Sat, Aug 25, 2018 at 7:34 AM, Jamie Rosenberg <[redacted]@google.com> wrote:
PRIVILEGED & CONFIDENTIAL

EXHIBIT 1386

Redacted - Privilege

Redacted - Privilege

On Sat, Aug 25, 2018 at 5:12 AM Edward Cunningham <[redacted]@google.com> wrote:
PRIVILEGED AND CONFIDENTIAL

Redacted - Privilege

On Sat, Aug 25, 2018 at 8:27 AM, Tristan Ostrowski [redacted]@google.com> wrote:
PRIVILEGED & CONFIDENTIAL

Redacted - Privilege

On Fri, Aug 24, 2018 at 10:58 PM, Shannon Newberry <[redacted]@google.com> wrote:
privileged and confidential

Thanks Lydia for this.

I sent a note to Android Central and TechCrunch with background points about how the 7 day disclosure is part of our standard policy (see below). Android Central just wrote back and said they'd link to our site with our vulnerability disclosure policy.

Marketplace wrote in asking for a comment and I shared our reactive statement and background points.

Will continue to monitor and push back against the claim we should have waited 90 days.

On Fri, Aug 24, 2018 at 10:19 PM, Lydia Ash [redacted]@google.com> wrote:
ATTORNEY CLIENT PRIVILEGED AND CONFIDENTIAL

Tristan - Please provide guidance.

EXHIBIT 1386-002

Pulled together an overview of what's out there now.
Techmeme
9to5Google
Android and Me
XDA Developers
Reddit
Slashdot
Ausdroid
Neowin
Pythom

Andrew Martonik who authored the original article gave some good coverage on Twitter
Another notable tweet

If helpful, internally I found this FAQ - https://sites.google.com/a/google.com/project-zero/disclosure

> *But what happens in other cases, such as when a vulnerability is fixed within deadline? Currently, we operate with the following guidelines:*
> *The bug is made public 7 days after patch availability. This extra courtesy time is actually another incentive for vendors to hit our deadlines.*
> *7 days after a vulnerability is public (either from Project Zero or elsewhere), it's fair game to public PoCs or exploits or detailed blog posts.*
> *As a matter of common courtesy, we should aim to send FYIs to vendors whenever we're about to publish new details on a public vulnerability. It's low effort, builds goodwill, and does not change your publication timeline.*

Also internally, the disclosure guidelines - https://g3doc.corp.google.com/company/teams/security-privacy/policies/security/guidelines/vulnerability-disclosure.md

Our external policy is not as explicit - https://googleprojectzero.blogspot.com/2015/02/feedback-and-data-driven-updates-to.html

On Fri, Aug 24, 2018 at 7:37 PM, Hiroshi Lockheimer <[redacted]@google.com> wrote:
Thanks. I think we should also talk about what we have done wrt devs in Play too, when they have violations etc

On Fri, Aug 24, 2018, 7:21 PM Shannon Newberry <[redacted]@google.com> wrote:
Hi all -

Yes, I'm actually sending a note to Android Central and my contacts at TechCrunch (they published) now. I'm going to point to this page and highlight this line specifically:

We notify vendors of vulnerabilities immediately, with details shared in public with the defensive community after 90 days, or sooner if the vendor releases a fix.

Trying to get a line from my security PR colleague right now to also help back up our point as well.

Stay tuned.

EXHIBIT 1386-003

On Fri, Aug 24, 2018 at 7:18 PM, Dave Kleidermacher <[redacted]@google.com> wrote:
Privileged

+1

Shannon, PLMK if I can help, happy to get on phone with media as needed over weekend or whenever. Don't think we should take those comments lying down since they are false and misleading security-wise.

DaveK

On Fri, Aug 24, 2018 at 6:22 PM Hiroshi Lockheimer <[redacted]@google.com> wrote:
If you don't mind (it is the weekend!) and also don't think it's a terrible idea, I think it would be good to get our points across ASAP. I worry if we wait until Monday we'll decide "oh the cycle has died down so let's not make any more news" but the issue with that is we would not have gotten our rationale across.

On Fri, Aug 24, 2018, 5:31 PM Shannon Newberry <[redacted]@google.com> wrote:
Privileged

I want to avoid getting into a back and forth with Tim, but I agree we need to defend this point.

I'll point reporters off-the-record to two things:

1) I agree it's worth finding some public examples in order to defend our 7 day decision and demonstrate this is typical practice. I'll work with Ed on this.
2) It also says in the bug (that Tim pointed to): *As mentioned via email, now the patched version of Fortnite Installer has been available for 7 days we will proceed to unrestrict this issue in line with Google's standard disclosure practices.* So I'll point people to that statement.

For now, I'm going to leave things as they stands unless something changes over the weekend. I can follow up with Android Central on Monday.

On Fri, Aug 24, 2018 at 5:11 PM, Hiroshi Lockheimer [redacted]@google.com> wrote:
Worth considering whether we reply back explaining for Play we typically do things on a much shorter time scale, and give examples. (Tim's point about 90 days is something I asked too, and it was explained to me -- and I agreed -- that for stuff on Play we typically do things quicker.)

On Fri, Aug 24, 2018, 4:51 PM Shannon Newberry <[redacted]@google.com> wrote:
Privileged

Tim just came out with a statement from Epic and blamed us for releasing this bug too quickly (copied statement below and its in the updated article by Android Central).

No inbound yet, but heads up in case Tim comes swinging next week.

If press ask I'll make it clear that we make bugs public 7 days after they are fixed as part of our typical disclosure practices.

Will keep this group posted if anything else changes.

Thanks,
Shannon

EXHIBIT 1386-004

Statement from Tim:

Epic Games provided the following comment from CEO Tim Sweeney:

Epic genuinely appreciated Google's effort to perform an in-depth security audit of Fortnite immediately following our release on Android,and share the results with Epic so we could speedily issue an update to fix the flaw they discovered.

However,it was irresponsible of Google to publicly disclose the technical details of the flaw so quickly,while many installations had not yet been updated and were still vulnerable.

An Epic security engineer,at my urging,requested Google delay public disclosure for the typical 90 days to allow time for the update to be more widely installed. Google refused. You can read it all at https://issuetracker.google.com/issues/112630336

Google's security analysis efforts are appreciated and benefit the Android platform,however a company as powerful as Google should practice more responsible disclosure timing than this,and not endanger users in the course of its counter-PR efforts against Epic's distribution of Fortnite outside of Google Play.

On Fri, Aug 24, 2018, 4:12 PM Lydia Ash [redacted]@google.com> wrote:
ATTORNEY CLIENT PRIVILEGED AND CONFIDENTIAL

Tristan - Please provide guidance.

Hey all - Notes from today's sync. Great way to end our week thanks to the heroics from Ed and Shannon!

Please take a look at the full notes below.

Going forward - the immediate fires are handled and we do not appear to need the daily sync to continue. However given the difficulty in getting time on cal and the possibility for something to still blow up in the press this meeting will stay on calendar temporarily. We anticipate the daily sync being cancelled, but will make that determination Monday afternoon based on latest information.
We will continue to monitor the Samsung side of this and the GPP policy and determine any followup conversations or meetings from that.

AI: ALL to weigh in if we need to keep daily standups or to come back together again. So far the group is in agreement to cancel.

ATTENDEES
Core task force: Colin Smith, Lydia Ash, Shannon Newberry, Mike Hochberg, Tian Lim, Purnima Kochikar, Tristan Ostrowski

MEETING NOTES

- **Epic** - Bug filed

○ Ed flipped the bug public just before 10am MTV time

○ Shannon has tipped off Android Central and the Security reporter at Wired. Things are moving slowly (it’s a Friday in August…). Android Central article will likely go today or over the weekend and then we forecast this will get picked up more on Monday.

○ The article went live during the sync - https://www.androidcentral.com/epic-games-first-fortnite-installer-allowed-hackers-download-install-silently

EXHIBIT 1386-005

- **Samsung** - bug filed
  - **PREVIOUS AI: DaveK** to check with security team as to if the Samsung problem is no longer a vulnerability. If Samsung is still a vulnerability, then we need to follow up with **Jamie/Purnima** on potentially flagging the Samsung installer.
  - **PREVIOUS AI: Purnima** to talk with Jamie should we ask Samsung if there are other installers similar to this?
  - **NEXT AI:** Waiting on mid-Sept for Samsung's push.
- **Installers** - Review anything that purports to be an installer Review for other mitd attacks (FN and Orange).
  - Ed and Purnima discussed BD contacts for the markets.
  - Ed: The info is included in this doc, and you can see an example of the bug I would be filing (that will eventually become public) there.

The app stores in question are:
9Apps: largest 3P app store (India, Brazil, Russia, Indonesia), owned by Alibaba.
Cafe Bazaar: main app store in Iran, and 2nd largest 3P store worldwide.
Aptoide: a somewhat popular 3P app store, also a complainant in various EU cases (+cc Michael FYI).

  - **AI: Ed** to link the bugs in this doc
- **GPP** - Decide how to harden GPP. Messaging is "GPP is getting more aggressive, and it will be felt if you do not do certain "good behavior" Android policy things.
  - go/off-market-enforcement
  - DaveK: Talked to Hiroshi today. He was OK on the general concept and asked that William continue to work on a specific proposal (we will tune the one in the go link and gather input from all here). In addition, he suggested we should consider even more out-of-box ideas on this. For example, we talked about the possibility of Pixel/Foo not allowing untrustworthy unknown sources at all (e.g. there could be a whitelist of approved non-Play sources that meet certain security requirements). His words in follow up after our meeting:
    - *Yes I think we should explore all kinds of options here to make it clear to our users when they are doing something insecure. Maybe we need to go further than "making it clear" and it requires us to rethink our stance. So I think it's worth brainstorming various ideas and exploring pros and cons.*

Redacted - Privilege

- **Public coverage**
  - Repeat from above Epic section
    - Shannon has tipped off Android Central and the Security reporter at Wired. Things are moving slowly (it's a Friday in August…). Android Central article will likely go today or over the weekend and then we forecast this will get picked up more on Monday.
    - The article went live during the sync - https://www.androidcentral.com/epic-games-first-fortnite-installer-allowed-hackers-download-install-silently
  - Reactive PR is prepped for further inquiries. No further outreach will be done.
  - **AI: Shannon** to continue to monitor.
- **Legal**

Redacted - Privilege

- **Going forward** - the immediate fires are handled and we do not appear to need the daily sync going forward. However given the difficulty in getting time on cal and the possibility for something to still blow up in the press this meeting will stay on calendar temporarily. We anticipate the daily sync being cancelled, but will make that determination Monday afternoon based on latest information.
  - **AI: ALL** to weigh in if we need to keep daily standups or to come back together again.

On Fri, Aug 24, 2018 at 3:32 PM, Hiroshi Lockheimer <[redacted]@google.com> wrote:
PRIVILEGED

Well done! Thank you.

On Fri, Aug 24, 2018 at 3:26 PM Shannon Newberry <[redacted]@google.com> wrote:
Privileged

We shared the bug with Android Central and worked with them today to shape a piece. The story is live: https://www.androidcentral.com/epic-games-first-fortnite-installer-allowed-hackers-download-install-silently

Great headline and outlines the points we wanted to convey.

We're not doing any additional outreach, but will monitor as this cycle kicks off.

On Fri, Aug 24, 2018 at 9:49 AM, Edward Cunningham <[redacted]@google.com> wrote:
Bug now external here: https://issuetracker.google.com/issues/112630336

(Note that if you view that URL with your corp account you'll be redirected to the internal Buganizer which shows more details than you'd see with a consumer account).

On Fri, Aug 24, 2018 at 12:53 AM, Shannon Newberry <[redacted]@google.com> wrote:
Privileged

Hiroshi - completely agree.

Ed - thanks for the update.

Once the bug is live tomorrow I'll tip off the reporters.

On Thu, Aug 23, 2018, 4:49 PM Edward Cunningham <[redacted]@google.com> wrote:
PRIVILEGED AND CONFIDENTIAL

I have informed the Epic security team (via email) that the bug will be made public tomorrow.

(Based on GPP data, a significant % of users have now installed/upgraded to the fixed version of the Fortnite Installer).

For general interest, here's what we've seen to-date for the number of daily Fortnite game installs since launch:

EXHIBIT 1386-007

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

On Fri, Aug 24, 2018 at 12:24 AM, Hiroshi Lockheimer [redacted]@google.com> wrote:
PRIVILEGED

Thanks. And speaking of goals, when we say we want to make "people aware" I think we are specifically talking about developers who may be considering going down this path. The message being security is super important and not always easy to achieve -- Play handles this for you, among other things (incl payments, featuring, merchandising, etc etc).

On Thu, Aug 23, 2018 at 2:59 PM Shannon Newberry <[redacted]@google.com> wrote:
privileged

+Hiroshi as FYI

Okay, so plan of action and next steps on the Fortnite security bug:

1) Ed needs to update the thread (ideally today) to notify Epic that we are going to make the bug public tomorrow now that it's been 7 days since they fixed it.
2) Bug goes live tomorrow morning 9 am PT
3) We tip off press about the bug and share our reactive statement and background points

Our goal here is to make people aware that we found a bug and validate the security concerns associated with Epic's decision, but we don't want to go too aggressively on offense given the current climate and tensions with Epic.

We'll explore a broader security narrative where we can highlight the work we do to keep users safe, but not bundle that with this bug.

I'll keep this group posted as things develop.

On Thu, Aug 23, 2018 at 12:05 PM, Purnima Kochikar <[redacted]@google.com> wrote:

EXHIBIT 1386-008

Privileged

My preference is to keep a channel open with Epic, given the importance of the Unreal Engine. As we did before, I will notify Mark, AFTER Ed has already notified Epic through the bug.

On Thu, Aug 23, 2018 at 11:38 AM Shannon Newberry <[redacted]@google.com> wrote:
Privileged and confidential

We were going to notify them through the bug. I don't see an issue with going directly to Mark. We would need to do it rather quickly if we're going to flip the bug to public tomorrow.

Ed - do you agree?

On Thu, Aug 23, 2018 at 11:30 AM, Jamie Rosenberg <[redacted]@google.com> wrote:
PRIVILEGED

For the heads up to Epic, is the team's thinking that we would do that through business channels (Mark Rein) or via Ed's security contact?

I've been looking for an excuse for us to connect with Mark and get his take on how things are going with their launch -- and also convey privately how much energy we're expending on this. If this is a moment to do that, Purnima and I can work through the details.

On Thu, Aug 23, 2018 at 9:45 AM Shannon Newberry <[redacted]@google.com> wrote:
Jamie/Sameer -

Yes we agreed yesterday to keep a more neutral approach to this specific security bug. Few reasons behind this:
1. When it comes to malware, we're not perfect on this issue and we should be careful how aggressive we are
2. Things in the press re: Fortnite are actually pretty positive for us. Press are already highlighting Epic's security risk, there's not a ton of benefit to us coming out very strongly and saying "see we told you this is risky and we found a vulnerability" -- it's just going to add fuel to a very contentious public story
3. As far as I'm aware, we've never been this aggressive with a bug before and the security team is worried about being politicized in this public fight

Finally, we can and should tell a broader security narrative, but I would do it beyond just Epic and the current situation. We could do it later as a way to demonstrate our overall efforts in security to keep users safe and use Epic as one point vs the main story.

So the recommendation is to:
*Make the bug public tomorrow and tipping on 2-3 reporters to start the cycle. We have a reactive statement and comms in place.
*Ed wants to give Epic a curtsey heads up that we will not give them 90 days before making this public but instead will publish the bug live tomorrow since the 90 days only applied to the timeframe to fix the bug.

EXHIBIT 1386-009

Happy to chat further today since I was OOO last week and we didn't get a chance to have you weigh in yesterday.

Thanks,
Shannon

On Thu, Aug 23, 2018 at 9:27 AM, Mike Hochberg [redacted]@google.com> wrote:
Will let Colin and Shannon weigh in but the thinking --- as I recall --- was that we were going to unlink the broader malware issue from the bug release. DaveK was connecting with Lookout to understand if/how they could expose some of the malware stats and that this could come later in the cycle.

On Thu, Aug 23, 2018 at 9:19 AM Sameer Samat <[redacted]@google.com> wrote:
yeah, same question as jamie re: the PR plan.

On Thu, Aug 23, 2018 at 9:02 AM Jamie Rosenberg [redacted]@google.com> wrote:
PRIVILEGED

FYI, this Twitter stream is pretty helpful:

https://twitter.com/stevesi/status/1032349824954159104

For the PR plan, if we're not using tomorrow to tell the broader story (number of fake apks we've blocked from other sites, etc.), is there a plan to do that in a different context?

Thanks

On Wed, Aug 22, 2018 at 9:20 PM Dave Kleidermacher <[redacted]@google.com> wrote:
Privileged & Confidential

○ **PREVIOUS AI: DaveK** to talk with Hiroshi. Proposal is stable. go/off-market-enforcement

Talked to Hiroshi today. He was OK on the general concept and asked that William continue to work on a specific proposal (we will tune the one in the go link and gather input from all here). In addition, he suggested we should consider even more out-of-box ideas on this. For example, we talked about the possibility of Pixel/Foo not allowing untrustworthy unknown sources at all (e.g. there could be a whitelist of approved non-Play sources that meet certain security requirements). His words in follow up after our meeting:

Yes I think we should explore all kinds of options here to make it clear to our users when they are doing something insecure. Maybe we need to go further than "making it clear" and it requires us to rethink our stance. So I think it's worth brainstorming various ideas and exploring pros and cons.

Redacted - Privilege

On Wed, Aug 22, 2018 at 3:55 PM Lydia Ash <[redacted]@google.com> wrote:
ATTORNEY CLIENT PRIVILEGED AND CONFIDENTIAL

Tristan - Please provide guidance.

Hey all - A number of updates to share with you all. We had the core team meet (notes) and have one key decision to draw your attention to. In evaluating all the options, it was decided to give Epic 7 days post-fix before releasing the bug publicly. This would technically mean the bug would be flipped on 8/23 at 4:12pm MTV time. Our plan of record is to have Ed flip the bug the morning of 8/24 LON time to approximate this. We will see if any coverage is picked up organically, and if not by 8am Friday MTV time Shannon will point a couple of friendlies at it.
Other notes are below including Ed's discovery of other similar issues in third-party app markets which will have bugs logged on them prior to making the Epic bug public.

Given no anticipated activity happening before the scheduled sync tomorrow, that has been cancelled. **Next sync will be Friday at 3pm**.

ATTENDEES
Core task force: Colin Smith, Lydia Ash, Shannon Newberry, Ed Cunningham, Mike Hochberg, Tian Lim

MEETING NOTES

- **Epic** - Bug filed

○ Shannon did the research with Ed and agreed to do either 7 or 14 days to public release - that would put it at going public either 8/24 or 8/31.

○ We could flip the bug Fri morning (8/24) and then point 3 friendlies at it, but not release any new metrics or data points. Could also have Lookout point to some other potential malware scams as a separate article and align to when the bug goes public - working on this with Lookout. We would likely need to feed that number to Lookout - DaveK is already on that thread. There is a small chance that Samsung could catch some bad press as it does specifically call out Samsung devices.

○ **Question: Mike and Tian** - are you good with pointing reporters at the bug? And to wait 14 days to do the flip to make it public? And ok with using Lookout to put out malware stat?

○ Not sure we trust Lookout to put the message out there exactly as we want. Not sure Lookout will position that we're earning out 30% - it could add more fuel to it.

○ Could let Lookout put their piece out there and eval the reaction.

○ **DECIDED: Ed** to flip the bug on 8/24 at early morning LON time (just past the precise 8/23 4:12pm 7 day extension), then **Shannon** can tip people off on Fri 8am if nobody has picked it up organically.

- **Samsung** - bug filed

○ **UPDATE** Samsung has provided additional perspective in the bug this morning - can see attached for their response

○ Ed: Essentially their writeup says that Samsung will make some changes to update the verifier in mid-Sept.

○ **PREVIOUS AI: DaveK** to check with security team as to if the Samsung problem is no longer a vulnerability. If Samsung is still a vulnerability, then we need to follow up with **Jamie/Purnima** on potentially flagging the Samsung installer.

○ **PREVIOUS AI: Purnima** to talk with Jamie should we ask Samsung if there are other installers similar to this?

EXHIBIT 1386-011

- ○ **NEXT AI:** Waiting on mid-Sept for Samsung's push.
- **Installers** - Review anything that purports to be an installer Review for other mitd attacks (FN and Orange).
- ○ Ed: We have other installers with issues - Indian app store and Iranian - so far we've found 3 of the largest third party app markets: 9 apps, apptoyed, cafe bazaar. The apps they download could be switched at the last minute. It's an identical vulnerability.
- ○

--

- The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

- Shannon Newberry
- Global Communications

[redacted]@google.com

[redacted]

If you received this communication by mistake, please don't forward it to anyone else (it may contain confidential or privileged information.) Please erase all copies of it, including all attachments, and please let me know it went to the wrong person. Thank you.

EXHIBIT 1386-012